REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
	Technical Report	-

4. TITLE AND SUBTITLE
Description and assessment of a user oriented approach for asymmetric threat detection

5a. CONTRACT NUMBER
W911NF-11-1-0176

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Valentina Dragos, Jürgen Ziegler, Paulo Costa

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
George Mason University
Office of Sponsored Programs
4400 University Drive, MSN 4C6
Fairfax, VA 22030 -4422

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
59841-MA.8

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
Asymmetric threats pose a difficult challenge to situational awareness systems. Current approaches for predicting or even detecting an asymmetric threat rely heavily on human knowledge, creating scalability issues due to the vast amount of data to be analyzed. Attempts to automate this process require a combination of advanced knowledge representation techniques to capture what human experts know about the domain and inferential reasoning approaches capable to work with incomplete, uncertain data. In our current research, we apply a verb-oriented ontology to capture actions, features, indicators, and other domain elements that are relevant to asymmetric threat

15. SUBJECT TERMS
asymmetric threat, Bayesian network, uncertainty; indicator, ontology, threat analysis, URREF criteria.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Paulo Costa
UU	UU	UU	UU		19b. TELEPHONE NUMBER 703-993-9989

Report Title

Description and assessment of a user oriented approach for asymmetric threat detection

ABSTRACT

Asymmetric threats pose a difficult challenge to situational awareness systems. Current approaches for predicting or even detecting an asymmetric threat rely heavily on human knowledge, creating scalability issues due to the vast amount of data to be analyzed. Attempts to automate this process require a combination of advanced knowledge representation techniques to capture what human experts know about the domain and inferential reasoning approaches capable to work with incomplete, uncertain data. In our current research, we apply a verb-oriented ontology to capture actions, features, indicators, and other domain elements that are relevant to asymmetric threat detection. Then, these elements are input to a Bayesian network that will calculate the posterior probability of a threat given the input. As in any complex process, evaluation is a key asset for ensuring that nothing is neglected and partial results are consistent with the expectations. This paper describes our approach for asymmetric threat detection and emphasizes how we are leveraging the Uncertainty Representation and Reasoning Evaluation framework (URREF), to support its evaluation. We discuss how the sources of uncertainty are identified and how we assess its impact to the outcome of the detection system.

TECHNICAL REPORT TR201312B
Description and assessment of a user oriented approach for asymmetric threat detection

Valentina Dragos
ONERA – The French Aerospace Lab
Palaiseau, France
valentina.dragos@onera.fr

Jürgen Ziegler
IABG Dept. CC30-C4ISR
Einsteinstr. 20 GE-85521 Ottobrunn
jziegler@iabg.de

Paulo C. G. Costa
George Mason University
Fairfax, VA, USA
pcosta@gmu.edu

Abstract— **Asymmetric threats pose a difficult challenge to situational awareness systems. Current approaches for predicting or even detecting an asymmetric threat rely heavily on human knowledge, creating scalability issues due to the vast amount of data to be analyzed. Attempts to automate this process require a combination of advanced knowledge representation techniques to capture what human experts know about the domain and inferential reasoning approaches capable to work with incomplete, uncertain data. In our current research, we apply a verb-oriented ontology to capture actions, features, indicators, and other domain elements that are relevant to asymmetric threat detection. Then, these elements are input to a Bayesian network that will calculate the posterior probability of a threat given the input. As in any complex process, evaluation is a key asset for ensuring that nothing is neglected and partial results are consistent with the expectations. This paper describes our approach for asymmetric threat detection and emphasizes how we are leveraging the Uncertainty Representation and Reasoning Evaluation framework (URREF), to support its evaluation. We discuss how the sources of uncertainty are identified and how we assess its impact to the outcome of the detection system.**

Keywords: asymmetric threat, Bayesian network, uncertainty; indicator, ontology, threat analysis, URREF criteria.

I. INTRODUCTION

Until a few years ago, the vast majority of research initiatives within the field of data fusion were focused on developing solutions for symmetric military warfare, in which equivalent forces were expected to comply with international conventions and international laws on warfare. As a result, models were created to describe components of the enemy forces or the processes used in their operations and field manoeuvres, see e.g. [15]. However, the emerging concept of asymmetric warfare (see e.g. [19] as first reference) became a major research subject, one that poses serious threats to both civilian and military facilities.

Asymmetric threat refers to circumstances in which a small group aims to destabilize a larger and more powerful group, while avoiding direct confrontation and using irregular forces. The asymmetric conflict is characterized by the absence of a formal conflict area and by the use of unconventional equipment: prohibited weapons, legitimate weapons employed in an unlawful way, improvised devices or even civilian facilities, cf. [17]. Actions conducted as a part of an asymmetric scenario are often illegal and make no distinction between civilian (or protected) and military targets. Asymmetric adversaries are unpredictable in their behaviour, and detection and prediction methods for regular warfare are usually not effective against them. New processing capabilities are needed to support intelligence analysis by retrieving patterns of hostile behaviour or clues of antagonistic intentions hidden in a large amount of harmless activity.

This paper presents a user oriented approach to detect and forecast asymmetric threats. The approach is based on Bayesian Networks (BN [5]) and has been developed for and is integrated to the AUGE (German acronym for "Automated Threat Detection") system, a demonstrator for automatic threat recognition built by IABG in a project sponsored by German Air Force's Transformation Centre [1], [2]. The project's goal was to provide automated support for J2 analysts to detect asymmetric threats. J2 analysts are responsible for the generation and assessment of the situational picture in large military units. An important aspect of the project was to ensure usability, taking into account the need to seamless combine the standard processes within the (GE) J2 organization with the experts' methodologies used to perform their reasoning and assessment processes. The paper is structured as follows: The next section presents approaches related to asymmetric threat analysis. Section III introduces our model for threat analysis, while section IV presents its formalization and the implementation of the user-centred approach. Uncertainties related to this approach are introduced in section V, and their assessment based on the URREF criteria is discussed in section VI. Conclusions and directions for future work end this paper

II. RELATED WORK

Asymmetric threat is an emerging concept, related to notions such as: hostile intent [16], hostile activities [12], suspicious activities [14] or even anomalies and

the so-called "out of ordinary" activities, e.g. [13]. Recently, the concept has been employed in an explicit manner by authors such as Singh et al. [14] and Valenzuela et al. [10].

One of the first solutions proposed to address asymmetric threats is the AHEAD (Analogical Hypothesis Elaborator for Activity Detection) approach described in [12]. Its authors developed a domain-independent method for hypothesis elaboration, taking structured evidence and hypothesis about the activities of an asymmetric adversary as input. The method's output is a semantic argument supporting or rejecting the hypothesis that combines case-based and analogical reasoning techniques. This solution is designed to assist the user in testing the hypothesis threat; and provides additional information in the form of arguments to ascertain the validity of the threat. While this work focuses on hypotheses elaboration, various solutions were proposed for asymmetric threat detection or prediction. Among them, Singh et al. consider the identification of asymmetric threats in relation to anomaly detection [13]. An anomaly is an event in which the distribution of observations is different before and after an unknown onset time. Hidden Markov models are used to model patterns of asymmetric threats, and a transaction-based probabilistic model allows for quick identification. Based on this approach, the ASAM (Adaptive Safety Analysis and Monitoring) system was developed in order to assist analysts to detect asymmetric threats and to predict possible evolutions of suspicious activities. The system is described in [14], while [17] explains its use to model terrorist events.

Genshe et al. propose a solution for asymmetric-threat detection and prediction based on advanced knowledge base and stochastic (Markov) game theory [11]. Asymmetric threats are detected and grouped by intelligent agents and their intentions are predicted using a decentralized Markov game model. The method exploits both domain knowledge and evidence about the current situation, while their solution is able to take into consideration the adversary's decision processes.

Several research efforts take a different perspective and aim to predict asymmetric threats by exploiting symbolic sources, such as intelligence reports. Chan et al. [9] proposed the ATRAP (Asymmetric Threat Response and Analysis Program), a set of tools for annotating and automatically extracting entities and relationships from documents. Once identified, these elements can be exploited to predict adversaries' future courses of action by creating situational threat templates and applying customized prediction algorithms.

Another solution based on templates is described in [10]. Authors developed a predictive model in order to automatically survey coded hypotheses (templates created by the intelligence community) by providing information assessment and confidence evaluation from non-numerical data. The predictive model is composed of different parts: information retrieval, assessment of the retrieved information; and score propagation. The model is traceable, transparent, and designed for human-in-the-loop data fusion.

In our approach, asymmetric threat analysis is considered a human-centred task, taking advantage of iterative interventions of various experts to create the most complete model. The solution is designed to support both hypothesis elaboration and asymmetric threat detection and prediction, by jointly exploiting domain knowledge and context issues. A verb ontology is used to model domain knowledge, making the approach easily adaptable to various application fields.

III. A MODEL FOR ASYMMETRIC THREAT ANALYSIS

This section introduces the main notions used for threat analysis.

A. Components of threat

The threat model highlights relevant components of threat and their weighted dependencies according to analysts' opinions. For this work, it is important to create a threat model that closely matches the mental model used by analysts when analysing possible threats. The model corresponds to the area of interest of analysts and defines a threat as a set of several components (or atoms). *Actors within the Own Area of Interes*t are organizations, groups or single actors considered as possibly threatening. An *Actor-Type* (or several *Actor-Types*) is assigned to each actor (e.g., terrorist or/and involved in organized crimes). An actor evolves within its *Area of Influence* (i.e. a geographic area or a cyber-area), and has specific *Actor-Intentions* (for instance "to drive away ISAF troops from Afghanistan" or "to get rich as fast as possible"). The intentions can be effectuated by choosing *Option for Action* (i.e. to perform a bomb attack at a market place**).** The *Option for Action* can be realised by performing a special *Action Chain*, which is created by a sensible sequence of *(Single) Actions***.** To perform the actions, the *Actor* must use available material and personnel resources.

According to the model above, analysts can elaborate statements describing a threat as follows: "A specific actor A pursues an Actor-Intention I and has chosen the Option of Action OA. For this purpose, his personnel Resources RP are performing the Action Chain AC with the Single Actions SA using the material Resources RM. The actor has the Actor-Type T and acts within his Area of Influence AI."

A complete description of threats is usually composed of several personal resources using various material resources to perform many single actions. A proposition of the analyst can restrict one or some single atoms of the threat.

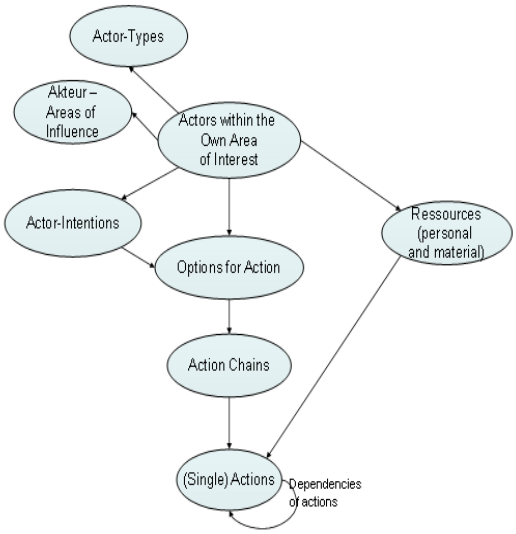

Figure 1 Atoms of threat and their dependencies

The atoms of the proposition are clearly not independent. Dependencies identified for this work, are described in Figure 1. Moreover, a qualitative weighting scheme is used to qualify each dependency as "very high", "high", "unknown", "low" or "very low". For example, the actor "TALIBAN" (organization) has a "very high" intention to drive away the ISAF troops from Afghanistan, but has a "very low" intention to get the Afghan government stabilized. It is possible that the same weight value will be assigned to several intentions of the same actor.

Tab. 1 describes the semantics of dependencies:

Dependency	**Semantics**
Actor within the Own Area of Interest -> Type	Type(s) assigned to actors
Actor within the Own Area of Interest -> Area of Influence	The actor has freedom of action in the area(s) of influence.
Actor within the Own Area of Interest -> Intention	Intentions of the actor.
Actor within the Own Area of Interest -> Option of action	Option for Action elected by actor. Actors often prefer special OAs against others.
Actor within the Own Area of Interest -> (personal or material) Resource	Resources (personal or material) available for actor
Intention -> Option of action	The option for action can be used to effectuate the intention
Option of action -> Action chain	The action chain can be used to realize the option of action.
Action chain -> Single action	The single action has to be performed in order to carry out the action chain
Single action i -> Single action k	The single action i has to be performed in order to perform the single action k.
Resource (personal)-> Single action Material resource -> Single action	The personal resource is able to perform the single action. The material allows performing the single action.

B. Indicators of threat

Indicators are defined as outcomes of intelligence sources conveying evidence for a particular threat. They correspond to conditions of suspicion, or "signatures" of threatening behaviour and several intelligence sources can be considered (HUMINT, SIGINT, IMINT and OSINT). The set of indicators offers a basis for searching evidence on threats. For instance, indicators for the atomic proposition for the action "Opponent reconnoitres the own camp by covert observation" could be: "Children are playing continuously in front of the camp" OR "A sales booth is implemented in front of the camp" OR "A person is regularly passing the camp" OR etc.

Users can define indicators for every atomic proposition of the threat. Most of the indicators are created for single actions or resources, but it is also possible to define other indicators (e.g. for intention to extract information from manifestos).

C. Hypothesis of threat

Hypotheses are assumptions that explain specific threats. An example of a hypothesis is "I guess the TALIBAN have the intention to unsettle the ISAF troops by choosing the course of actions IED attack together with subsequent assaults". A semi-automated approach, described below, was developed to support experts modelling and analysts detecting threats.

IV. A USER-CENTRED APPROACH TO DETECT THREATS

We propose a general architecture for asymmetric threat detection allowing different types of users to model various threats, to identify threat indicators, and to elaborate and test several hypothesis explaining threats.

A. Using Bayesian network (BN) to model threats

For this work, BNs are used to model threats composed of several correlated atoms. This formalism is appropriate as it allows taking into account causal dependencies of threat atoms and use the mutual exclusivity of some parts of the threat model in order to "declare away" competing propositions. For usability reasons, it is necessary to generate the Bayesian model automatically, since users cannot define and deal with large BNs composed of several hundreds of nodes. Weights assigned by users to dependencies between atoms of threat are translated to conditional probability tables (CPT), and their semantics is preserved.

The structure of the BN is generated from the threat model by considering the fact that a single threat requires multiple resources and can be composed of several "single actions." Resources and actions are translated into multiple binary non-exclusive nodes. The structure of the BN associated to a threat model is sketched in Fig.2.

By using BNs to model threats, algorithms required to support analyst's tasks are selected from the BN algorithm's toolset.

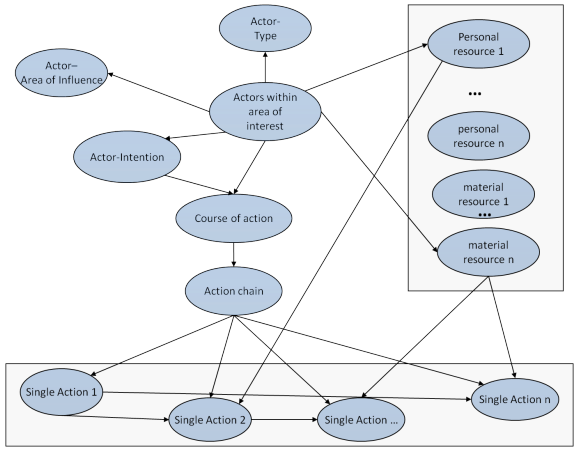

Fig. 2 Bayesian Network for threat detection

B. *Formalization and identification of indicators [2]*

A verb-based ontology provides a formal model for indicators. Verbs are considered important for this approach as threat-evidence is related to activities of opponents. The ontology highlights verbs and their associated frames to model relevant actions of opponents and their associated context. By using the ontology, an indicator is modelled as a set of several verbs together with their corresponding frames [7].

The formal model of an indicator comprises one or several verbs from the ontology together with their verb-frames, which can be filled with additional qualifications to sharpen the restrictions to be matched by source information. Indicators are identified from textual information by algorithms using linguistic methods along with the ontology of verbs. Those algorithms extract information from texts and translate it into verb frames. Therefore, it is possible to compare this representation to indicators defined in a similar manner. An indicator can be matched exactly by the information, or partially when the structure of the ontology has to be used to get the match (e.g. an indicator scheme contains a red Mercedes and the associated result of source information contains a red car at the same part of the scheme).

C. *Elaboration of hypothesis*

Hypotheses are elaborated for both model and indicators. Some hypotheses are related to specific states of the model, and in this case it becomes possible to trigger changes of the model itself. When related to indicators, a hypothesis allows to check their impact on probability values of the BN modelling the threat.

D. *User-centred identification of threats*

In order to identify asymmetric threats, various types of users interact with the model in order to achieve several tasks, as described hereafter.

Subject matter experts (SME) define and maintain their specific part of the threat model. Usually, they have knowledge about particular factors, e.g. some SME knows "everything" about weapons and their distribution in Afghanistan. The design of the threat model allows for several SME to improve the model by adding their knowledge regardless of one another. However, a supervisor is in charge of monitoring the generation of the threat model, and it can perform causal analysis in order to check the consistency of the model.

The source specific experts are responsible for the definition of the indicators and the generation of indicator matches using the methodology described above.

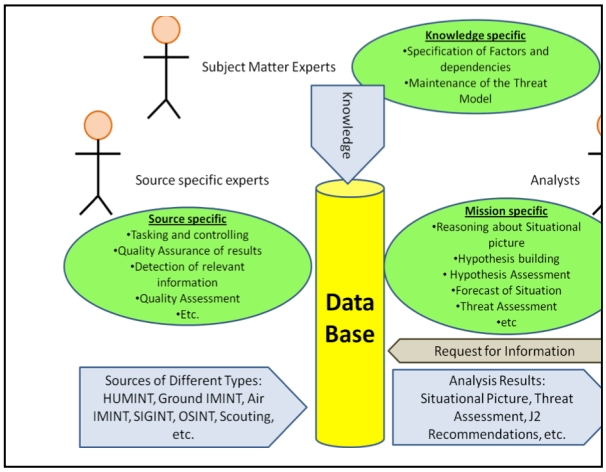

Fig. 3 A user-oriented approach to model and detect threats

While subject matter experts create the threat model, source specific experts provide indicators to assess evidence of one or more elements of the model. Therefore, they can change the model or one of its states.

Analysts use the threat model, including the indicators, to perform causal analysis of the model, carry out a diagnosis and build and assess different hypothesis explaining the threat.

The goal of causal analysis is to assist in comprehending different factors of threats along with their dependencies. It can also support the generation of hypothesis concerning possible threats. A diagnosis is performed in order to identify and predict threats, thanks to a continuous assessment of the situation. The diagnosis is calculated using the evidence generated by the indicator matches. Alerts are triggered if significant probability values are assigned to some atoms of the threat. The diagnosis offers a means for a long term analysis of threats.

Analysts can also elaborate hypotheses about threats, by setting a priori values to different appropriate states of the model, or hypotheses about evidences by

assigning a priori values for indicators. Hypotheses can also be related to the structure of the model and can trigger the insertion of new components or the elimination of existing ones. Analysts can also assess the hypotheses by taking into account both contradictions or confirmations of hypotheses with respect to evidence and/or domain knowledge.

V. Uncertainty Model of Threat Identification

The process of threat identification using the user-oriented approach previously described is affected by different types of uncertainties. These include the quality of indicators or evidence pieces, the way knowledge is handled by the system, and the form adopted to deliver outcomes to users, see fig. 4.

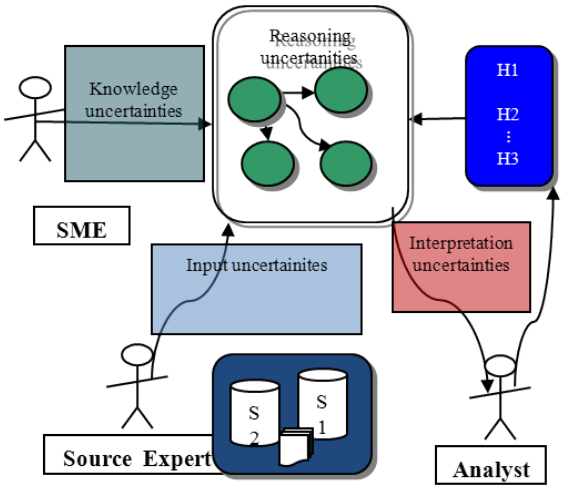

Fig. 4 Uncertainty model of threat detection

A. *Uncertainty of inputs*

For the threat analysis, indicators are input data, and are represented as binary evidence nodes of a Bayesian network. They are extracted from data by using pattern-matching approaches that usually provide uncertain results. Therefore, the BN is enriched thanks to so called "soft evidence" [4], in the form of a probability value p assigned to each indicator node, whose semantics is as follows: "The proposition represented by the indicator is true with probability p." The probability value is set by considering both the perfect and imperfect matches of the indicator (see [3]), and the quality of its sources. A value p = 0.5 means "no indicator match" due to the binary character of the evidence node. Therefore it is also possible to use information contradicting the indicator to get probabilities less than 0.5.

B. *Uncertainty of knowledge handling: Weighted Expectations [3]*

Expert knowledge is used to generate CPTs for the BN, by adopting the "scale based distribution retrieval." This is a two-step approach: first, weight values defined by users are transformed into scale values, which are predefined values between 0 and 1. The translation is carried out by preserving the sequence and the distance of the weights according to the meaning of qualitative values. In the second step, the resulting table column values are normalized. For dependencies of factors with many states, the normalization step leads to small numerical values, even if the qualitative value of the dependency was "very high".[1]

CPTs reflect the dependencies between states of two nodes. To finalize the CPT, the probability of nodes having more than one parent is estimated by multiplying dependency tables of the considered nodes. In this case, the domain expert indicates the type of parent node (e.g. the material resource, the personal resource or the action chain as parent nodes of the single actions) having more or less influence on the dependent node.

For this approach, special cases are dependencies between nodes of the threat model and nodes corresponding to indicators. The semantics of such dependencies is: "If the state of the node is … then an indicator match should be detected". At the BN level, this is represented by an oriented connection, going from threat node to indicator node, while the weight of this dependency and the calculation of CPT are as already described. It is important to keep in mind that the CPT represents weighted expectations, and no "real" probabilities.

C. *Reasoning uncertainties*

For this approach, various states of the BN represent the assessment of one threat. Moreover, every node of the BN has a discrete probability distribution. Some nodes have multiple exclusive states e.g. for "actor within area of interest"; binary nodes correspond to personal and material resources and to single actions as well. States of nodes represent propositions of threat atoms, and propositions about a threat are therefore created by combining them.

Thus, reasoning uncertainties are related to the capacity of the system to handle complex BNs and provide accurate results within a reasonable amount of time.

D. *Outcome related uncertainties: weighted threat factors*

Output uncertainties are due to transformations required to create the outcome and to provide this outcome in a user-friendly form. After creating the weighted BN, diagnostic algorithms are used to compute probability values of node states. The relative probability value of an atom is given by the calculated

[1] This should not annoy the BN expert, but it might puzzle domain experts.

probability distribution. The relative probability of a threat is computed by combining the probabilities of its atoms respectively. Thus, the most probable and also most improbable threats can be easily extracted. The results of the calculations are considered as weighted threat factors and have to be re-translated into the qualitative values of the user weights, in order to provide a user-friendly form of results as statements such as: "It is very probable that the actor x is responsible for the considered threat and its intension is to …".

VI. ASSESSMENT OF UNCERTAINTY USING URREF

In this chapter the described approach is analysed based on measures defined by the uncertainty representation and reasoning evaluation framework (URREF), which is depicted in Figure 5. In URREF[2], criteria quantify each type of uncertainty previously identified and directions to evaluate them are proposed. Because the approach has a strong focus on usability and traceability of results, the related criteria are of special importance.

The described approach is designed so that the data used for the fusion is defined by the users. Therefore, the analysis of the approach is restricted to the discussion whether it can cover and handle the relevant uncertainties. If the approach is applied in a real environment it is expected that the configuration data of the model will continuously be improved by the SME and source experts by discussing the results of the system in interaction with the analyst.

It is therefore necessary to use a data set covering a relatively long scenario period to evaluate the system with experimental scenario and data. As a consequence, a large data set is required. Nevertheless, the presented analysis of different uncertainty levels associated to various elements of this model allows us to have a first assessment of the overall process.

A. Criteria for input related uncertainties

Those criteria are intended to qualify indicators provided by analysts when analysing threats. Each indicator is assessed incrementally, using values of credibility and relevance to the problem.

Credibility is a value of source information, which is the basis of the calculation of indicator matches. The credibility of information is usually provided by its origin. If an indicator match is calculated based on source information, its credibility is passed on to the indicator match. An evaluation scheme can be used to enable different analysts to evaluate indicators in a similar manner. For instance, NATO standard [8] can be used to assess indicators provided by HUMINT data.

[2] The URREF ontology is available at http://eturwg.c4i.gmu.edu

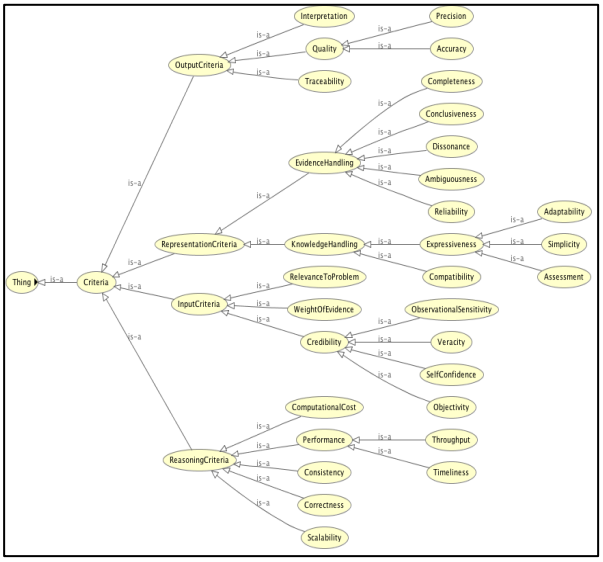

Fig. 5 The URREF Ontology

Indicators have different degrees of relevance to the problem. Firstly, they are created by a complete or partial match of the information and the pattern defined. Secondly, the CPT linking the atom of the threat model to the indicator also represents the SME assessment of the indicator match's relevance. Hence, if an indicator match arises; it is also possible to estimate its relevance to the problem.

The approach provides an internal functionality used to improve the accuracy of input uncertainties. If there is an indicator match the system can present the original information for a selected indicator match together with the information extracted using the linguistic approach. It can be used by experts to assess whether the described values are adequate which enables the experts to adapt them.

B. Criteria for uncertainties concerning knowledge handling

The criteria for knowledge-handling are relevant to assess the way SMEs create the threat model thanks to their domain knowledge. This was one of the most important requirements of the approach. We discuss adaptability and simplicity because they are the most relevant criteria for the usability of the knowledge handling.

"Adaptability criteria encompass the ability of the representational model to allow for different configurations of it. As an example, an adaptable representational framework would have most of its elements configurable by Subject matter Experts (SME)[20]".

The approach can be continuously adopted during its use in a special mission taking into account the evolving knowledge of the SME. Additionally the

model should also be easily adaptable to different types of missions, e.g. Congo and Afghanistan. Finally the described approach is adaptable not only to asymmetric threat applications but to all applications having the same structure of the threat model, e.g.. to organized crime and homeland security applications as well.

Simplicity: "This refers to the ability to use the uncertainty management capability, e.g., to execute common operations (configure the system, enter evidence, proceed with analysis, etc.) without requiring deep knowledge about the inner details (mathematical underpinnings of the inferential process, algorithmic details, etc.)" (Rewording of definition by Kathryn Laskey) [20] This was one of the approach's key features as described in chapter IV.

C. *Criteria for reasoning related uncertainties*

Reasoning criteria are intended to capture both the quality of the model created by different experts and to provide a means to evaluate the inference process performed for threat detection.

First, the model can be characterized by its dissonance, which occurs as model is created and used by different actors. For instance, dissonance becomes relevant when different sources provide contradictory information or when different experts change the model in a way that different parts of the model become inconsistent. As BN are used to model threats, the level of dissonance can be estimated by using BN tools.

Inferences used to detect threats are assessed by their scalability, computational cost and timeliness. Scalability is intended to capture the size and the complexity of the BN. For this approach, the structure and the number of the threat model's factors are constant, but nodes have an important number of states and are connected by numerous dependencies. Therefore, values of scalability can be estimates by taking into account the number of BN nodes and the density of its links.

The computational cost is related to BN intrinsic performances, and it can be important for BN having important sizes.

Timeliness is an important aspect to be considered when the system is used interactively for hypothesis generation and assessment. This measure is related to BN intrinsic performances and to the complexity of the task performed.

D. *Criteria for output related uncertainties*

Results of this approach are in the form of assertions describing both the threat and its associated probability.

Therefore, precision, interpretation and traceability are criteria describing the outcome.

A high level of precision allows users easily identifying the most probable threats. Even if the described translation of the BN's probability values to qualitative attributes of the user model decreases the precision of results, this translation is necessary as intuitively users encounter difficulties while analysing not clearly differentiated values of probabilities.

Interpretation is a key factor for a user-oriented approach. The approach is designed to provide results in a user-friendly form by translating the calculation results into the user model. Therefore the outcomes can easily be interpreted and compared.

Traceability of results is an important aspect for asymmetric threat applications, as the user has the entire responsibility of the outcome provided and therefore needs to check the final result manually before making further use of it. Traceability is firstly obtained by using BN. Additionally the approach is designed in a way that the user is able to check if the result is sensible by presenting the original information, the indicator matches and the causal relations, which are the reasons for the final result.

VII. CONCLUSION AND FUTURE WORK

This paper presents a user-oriented approach developed for asymmetric threat(s) detection. User integration is considered a key feature to perform asymmetric threat analysis in order to provide an approach through which the user will trust in the fusion results. The approach aims to detect threatening insights out of enormous amounts of noisy, scattered and partial data. Our solution is based on Bayesian Networks, and exploits domain knowledge in order to extract indicators. We also discuss the uncertainty model related to our approach and discuss the assessment of uncertainty by using URREF criteria.

Performing human-in-the-loop evaluation and validation is a direction for future work. A set of real data or a scenario with realistic data sets will be used, and results of the approach will be compared to evolving reality. The main assessment criterion will be: "Does the approach improve the capability of users to detect threats." For this validation process, URREF criteria can be used in order to receive a more detailed analysis of results. This detailed analysis can be applied to the different parts of the approach and to the intermediate results of the threat analysis.

Future work could also consist of improvement of the approaches' results, thanks to the assessment of uncertainty criteria. In this case, uncertainty criteria will be used to evaluate the relevance of different elements of the model in order to ignore non-relevant features, which could improve the accuracy of the solution.

An additional promising application of the URREF criteria is the development of a quality assurance

functionality to be used by the persons which are responsible to assure the quality of the threat model. As already described the threat model is adapted by different person with different responsibilities during its usage. There is an inherent danger, that the model becomes worse due to changes e.g. by adding inconsistent and / or redundant domain knowledge. URREF criteria can be calculated to support quality managers to detect degradations of the model quality.

A different direction for future work concerns the improvement of techniques used to extract indicators. For instance, user interventions required to validate the extracted information could be used to provide additional information about their quality, which can be taken into account by the system automatically.

ACKNOWLEDGMENTS

The Army Research Office provided partial funding to Paulo Costa for this research, under grant W911NF-11-1-0176.

REFERENCES

[1] Markus Bresinsky, Frank Detje, Nane Kratzke, Ulrich Schade, Jürgen Ziegler. Konzept Automatisierte Gefahrenerkennung, Annex 2 of Final Report of the Study. 2009

[2] Markus Bresinsky, Ulrich Schade, Jürgen Ziegler. Methodische Grundlagen zur Umsetzung des Konzepts "Automatische Gefahrenerkennung", Annex 2 of Final Report of the Study. 2009 (Title in English: Methodical Foundation for the Realization of the Concept "Automatic Threat Detection")

[3] Bastian Haarmann & Lukas Sikorski, Jürgen Ziegler: Applied Text Mining for Military Intelligence Necessities, Proceedings of the 6th Future Security Conference, Berlin, Germany, 2011.

[4] Jürgen Ziegler, Bastian Haarmann: Automatic Generation of Large Causal Bayesian Networks from User Oriented Models, in proceedings of the 6th Workshop on Sensor Data Fusion Berlin, Germany, 2011.

[5] Judea Pearl. Probabilistic Reasoning . in Intelligent Systems: Network of Plausible Inference Morgan Kaufmann Publishers Inc. Revised Second Printing 1998

[6] Thomas L. Saaty: Relative Measurement and Its Generalization in Decision Making. Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors (The Analytic Hierarchy/Network Process) Rev. R. Acad. Cien. Serie A. Mat. VOL. 102 (2), 2008, pp. 251–318

[7] Faure, D. and Nedellec, C. : A corpus-based conceptual clustering method for verb frames and ontology, In p. Velardi, editor, Proceedings of the LREC Workshop on adapting lexical and corpus resources to sublanguages and applications, 1998.

[8] NATO STANAG 2511, Intelligence reports, 2003

[9] Erwin Chan, Jason Ginsburg, Brian Ten Eyck, Jerzy W. Rozenblit, Mike Dameron. Text analysis and entity extraction in asymmetric threat response and prediction. In Proceedings of the 2010 IEEE International Conference on Intelligence and Security Informatics, ISI'2010. pp.202~207

[10] Michael L. Valenzuela, Chuan Feng, Praneel Reddy, Faisal Momen, Jerzy W. Rozenblit, Brian Ten Eyck, Ferenc Szidarovszky, "A Non-numerical Predictive Model for Asymmetric Analysis," ecbs, pp.311-315, 2010 17th IEEE International Conference and Workshops on the Engineering of Computer-Based Systems, 2010

[11] Genshe Chen; Shen, D.; Chiman Kwan; Cruz, J.B.; Kruger, M.; , "Game Theoretic Approach to Threat Prediction and Situation Awareness," *Information Fusion, 2006 9th International Conference on* , vol., no., pp.1-8, 10-13 July 2006

[12] J. William Murdock, David W. Aha , Leonard A. Breslow AHEAD: Case-Based Process Model Explanation of Asymmetric Threats, Naval Research Laboratory, Technical report, 2002.

[13] Singh, S.; Haiying Tu; Donat, W.; Pattipati, K.; Willett, P.; , "Anomaly Detection via Feature-Aided Tracking and Hidden Markov Models," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* , vol.39, no.1, pp.144-159, Jan. 2009 doi: 10.1109/TSMCA.2008.2007944

[14] Singh, S.; Donat, W.; Haiying Tu; Jijun Lu; Pattipati, K.; Willett, P.; , "An Advanced System for Modelling Asymmetric Threats," *Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on* , vol.5, no., pp.3943-3948, 8-11 Oct. 2006 doi: 10.1109/ICSMC.2006.384748

[15] J. Llinas, C.L. Bowman, G. Rogova, A. N. Steinberg, E. Waltz and F.E. White: Revisiting the JDL data fusion model ll, In Proceedings of the 7th International Conference on Information Fusion, Stockholm, Sweden, 2004.

[16] A. Pawlowski, S. Gigili and Franck Vetesi: Situation and threat refinement approach for combating the asymmetric threat, Military Sensing Symposia, National Symposium on Sensor and Data Fusion, San Diego, USA, 2002.

[17] Non-Lethal Weapons and Future Peace Enforcement Operations, NATO RTO Technical Report TR-SAS-040, 2003.

[18] Singh, S.; Donat, W.; Haiying Tu; Jijun Lu; Pattipati, K.; Willett, P.: Stochastic Modelling of a Terrorist Event via the ASAM system, IEEE Conference on *Systems, Man and Cybernetics, Netherlands, 2004.*

[19] Counter insurgency warfare: Theory and praxis. David Galula (1964, Reprint 2006)

[20] Definition and discussion of the URREF ontology and its criteria (http://eturwg.c4i.gmu.edu/, http://eturwg.c4i.gmu.edu/?q=URREF_Ontology, http://eturwg.c4i.gmu.edu/?q=Forum_EvaluationProcedures